REMARKS

Applicants have thoroughly considered the Examiner's remarks in the January 22, 2008 Office action. This Amendment B amends claims 1, 16, 26, and 33. Claims 1-3, 5-24, and 26-40 are thus presented in the application for further examination. Reconsideration of the application as amended and in view of the following remarks is respectfully requested.

At page 2 of the Office action, the Examiner indicates that the phrase "means for" appears within claims 25 and 32 and considers 35 U.S.C. § 112 paragraph 6 to be invoked. Claim 25 has been canceled. Applicants acknowledge that the "means for" language appears in claim 32 and that the cited section of the U.S.C. is therefore invoked with respect to claim 32.

Applicants note that the paragraph numbers in the Application as published (U.S. Publication No. 2005/0216955) do not match the paragraph numbers in the Application as filed. For purposes of discussion in this Amendment B, all paragraph numbers cited herein refer to the paragraph numbers in the Application as published.

No New Matter

Claims 1, 16, and 33 have been amended to recite that the memory area or database storing incorrect usernames and passwords is included in the user authentication system which was inherent in claim 26 as originally presented. Thus, no new matter is presented herein since the subject matter appeared in the claims as originally presented.

Claim Rejections Under 35 U.S.C. § 101

Applicants acknowledge that the Examiner has withdrawn all of the claim rejections under 35 U.S.C. § 101.

Claim Rejections Under 35 U.S.C. § 103

Claims 1-3, 5, 8-10, 13-17, 20-22, 26-27, 29, 30, 32-34, 36-38, and 40 stand rejected under 35 U.S.C. § 103 as being unpatentable over U.S. Patent Application Publication No. 2003/0145225 by Bruton, III et al. (hereinafter Bruton) in view of U.S. Patent Publication No. 2004/0059941 by Hardman et al. (hereinafter Hardman). Applicants respectfully submit that the cited references fail to teach or suggest each and every element of the invention as claimed.

Bruton teaches an intrusion detection system (IDS) that is incorporated at multiple layers within a host computer. The IDS includes packet sniffing and scanning technology (see Bruton at paragraphs [0046]-[0052]). The IDS creates a log of received data packets and checks the log for attack signatures in order to determine an intrusion attack (see, for example, Bruton at paragraph [0060]). Bruton logs packets received at a host **regardless of the contents of the packets**. Bruton fails to teach redacting a password of a request from a memory if the request is successful. In other words, Bruton fails to teach storing a password and username of a login attempt in a memory of the authentication service **only if the login attempt is unsuccessful**.

Hardman teaches a user authentication system including a central authentication system and third party servers. The third party servers provide authentication requests from users to the central authentication system and receive approvals or denials from the central authentication system in response. When an authentication request is denied, the third party server stores the failed username and password. Thereafter, the third party server does not forward any request identical to the stored username and password in order to avoid unnecessary traffic and authentication attempts at the central facility (see Hardman at paragraphs [0011]-[0016] and [0064]). Hardman fails to teach storing a password and username of a login attempt **in a memory of the authentication service only if the login attempt is unsuccessful**. Storing the username and password of failed authentication requests at the third party servers of Hardman does not create a database of authentication attempts available to the authentication service for detecting an attack. To the contrary, this aspect of Hardman is directed to reducing traffic between the third party servers and the central authentication service (see Hardman at paragraph [0064]). **This fragments the authentication request data across multiple third party servers** and reduces the central authentication facility's access to the data, limiting the ability of the central authentication database to detect an attack. Hardman addresses an entirely different problem than the present application. Hardman provides a system that enables a user to log in at multiple third party servers by logging into one of the third party servers by logging into and storing a cookie from a central authentication service. Hardman also teaches methods for minimizing traffic between the third party servers and the central authentication service at paragraphs [0013] and [0064]. Hardman does not address detecting an attack on the central authentication service or securing the central authentication service in any way.

In contrast, aspects of the present invention include employing discretion when logging authentication and/or logon requests in a database of the authentication service. The failed authentication requests are stored **in a database of the authentication service** so that the authentication service can access and analyze the failed requests for patterns to detect an attack. Additionally, storing **only failed authentication and/or logon requests** and not this information from any successful requests prevents the authentication service from producing an additional database target for attack from hacking or the like. When a server receives a request, the authentication server (or a cooperating group of servers comprising the authentication server) determines whether the request is successful (e.g., whether the request contains a corresponding account and password) and only logs a password associated with the request in a database of the authentication service if the request is unsuccessful (see Application at paragraphs [0009]-[0010], [0028]-[0031], and [0036]-[0037]). That is, it is desirable to minimize the number of sources storing valid authentication and/or logon data in order to minimize the risk of a successful attack, while keeping attempted logon data (i.e., authentication request data) available to the authentication service in order to enable the authentication service to detect an attack in progress. To this end, claim 1 recites, "...storing data relating to a plurality of requests communicated to an authentication service from a plurality of user agents via a data communication network, said requests each including a password, and wherein storing the data relating to the requests comprises **storing the password of each of the requests in a database of the authentication service only if the request is unsuccessful**...." Claim 16 recites, "...a first memory area to store data relating to a plurality of requests communicated to an authentication service from a plurality of user agents via a data communication network, said data being stored in the first memory area as a log of the authentication service, wherein each of the requests communicated to the authentication service includes a password and wherein **the stored data contains the password of each of the requests only if the request is unsuccessful, and wherein said first memory area is a database of the authentication service**...."

Claim 26 is directed to user authentication system that receives authentication requests from a plurality of user agents. According to this claim, "...a first memory area to store data relating to a plurality of unsuccessful requests communicated from the plurality of user agents, wherein **the stored data ... does not include the password of any successful requests, wherein the first memory area is a database of the user authentication service** ...." The

storage media of claim 33 comprises "a memory component to store data relating to a plurality of unsuccessful requests communicated to the authentication service from the plurality of user agents, wherein **the stored data includes the password of each of the unsuccessful requests communicated to the authentication service and does not include the password of any successful requests, wherein said memory component comprises a database of the authentication service** …."

None of the other cited references cure these defects. Applicants submit that claims 1, 16, 26, and 33 are therefore allowable over the cited art. Claims 2-3, 5-15, 17-24, 27-32, and 34-40 depend from these claims and are allowable over the cited art for at least the same reasons. Applicant therefore requests that the Examiner withdraw the rejection of these claims.

Claims 4, 6, 7, 18, 19, 28, and 35 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Bruton in view of U.S. Patent Publication No. 2003/0009693 by Brock et al. (hereinafter Brock) in further view of Hardman. Brock discloses counting logon failures and suspecting an intrusion if the number of failures exceeds a threshold over a given period of time. The cited portion of Brock does not disclose storing a password relating to a request at all, much less only storing the password in a database of the authentication service if the request is unsuccessful. Brock therefore fails to cure the defects of the cited references with respect to independent claims 1, 16, 26, and 33 as discussed above. Claims 4, 6, 7, 18, 19, 28, and 35 depend from these claims and are allowable for at least the same reasons as the claims from which they depend.

Claims 11, 12, 23, 24, 31, and 39 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Bruton in view of Hardman in further view of U.S. Patent Publication No. 2002/0097145 by Tumey et al. (hereinafter Tumey). Tumey teaches a vehicle security system using facial image verification. Tumey fails to cure the defects of the cited art with respect to independent claims 1, 16, 26, and 33 as discussed above. Claims 11, 12, 23, 24, 31, and 39 depend from these claims and are allowable for at least the same reasons as the claims from which they depend.

Conclusion

Applicants submit that the claims are allowable for at least the reasons set forth herein. Applicants thus respectfully submit that claims 1-3, 5-24, and 26-40 as presented are in condition for allowance and respectfully request favorable reconsideration of this application.

Although the prior art made of record and not relied upon may be considered pertinent to the disclosure, none of these references anticipates or makes obvious the recited aspects of the invention. The fact that Applicants may not have specifically traversed any particular assertion by the Office should not be construed as indicating Applicants' agreement therewith.

Applicants wish to expedite prosecution of this application. If the Examiner deems the application to not be in condition for allowance, the Examiner is invited and encouraged to telephone the undersigned to discuss making an Examiner's amendment to place the application in condition for allowance.

The Commissioner is hereby authorized to charge any deficiency or overpayment of any required fee during the entire pendency of this application to Deposit Account No. 19-1345.

Respectfully submitted,

/Robert M. Bain/

Robert M. Bain , Reg. No. 36,736
SENNIGER POWERS LLP
One Metropolitan Square, 16th Floor
St. Louis, Missouri 63102
(314) 231-5400

RMB/MAP/lav